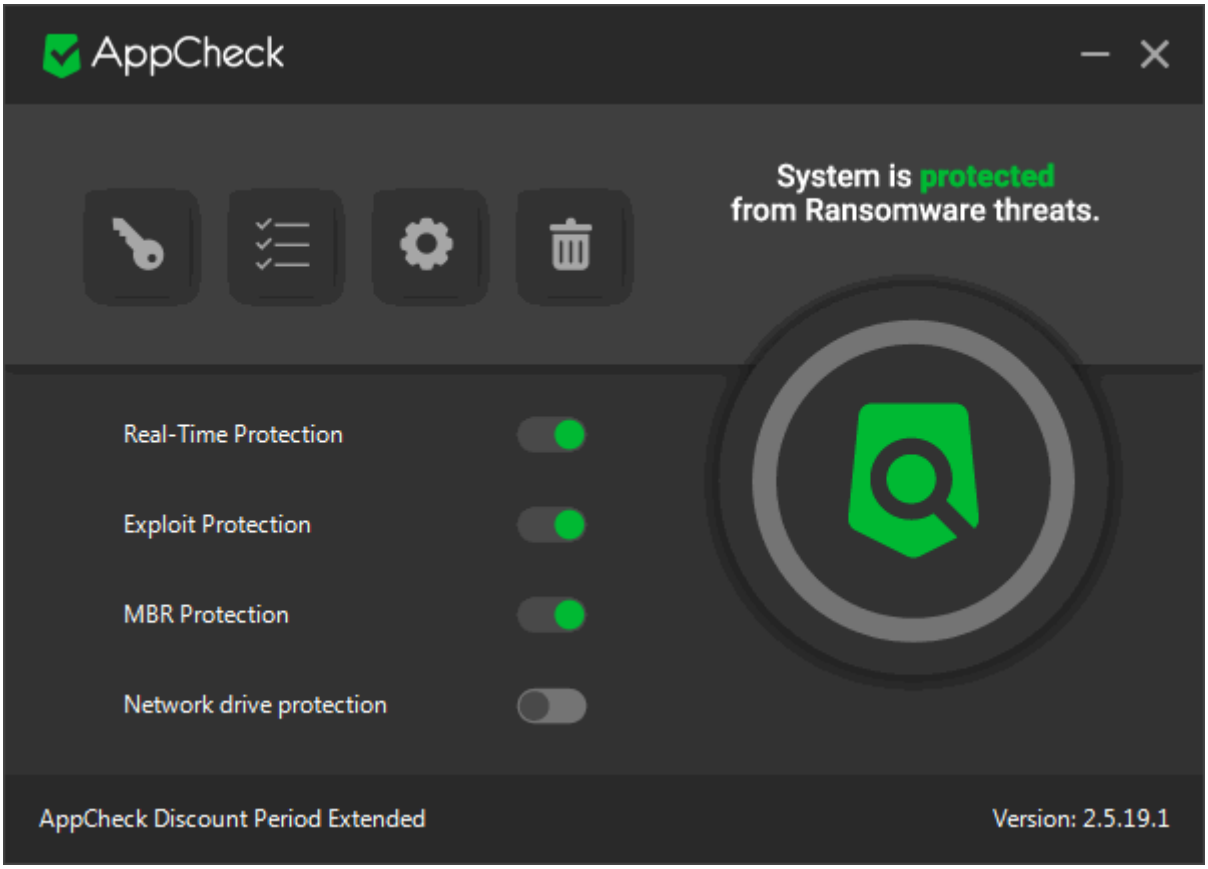
AppCheck Anti-Ransomware v.2.5

AppCheck Anti-Ransomware è un software progettato per prevenire attacchi ransomware. Esegue il monitoraggio del sistema bloccando automaticamente la maggior parte della crittografia ransomware e mantenendo un backup dei file originali in una directory protetta, consentendo di eseguire il ripristino delle modifiche apportate. Include: Cleaner per rimuovere malware noti e PUP / PUA. Exploit Guard protegge le vulnerabilità dei browser Web e delle applicazioni. Protezione MBR / GPT protezione da ransomware e malware che modificano l'MBR.

<**Clicca qui**> per scaricare **AppCheck Anti-Ransomware**

Articolo modificato, **clicca qui** per la voce aggiunta.

Cos'è un Ransomware? Un **Ransomware** è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione. Ad esempio, alcune forme di ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro. Continua su Wikipedia.

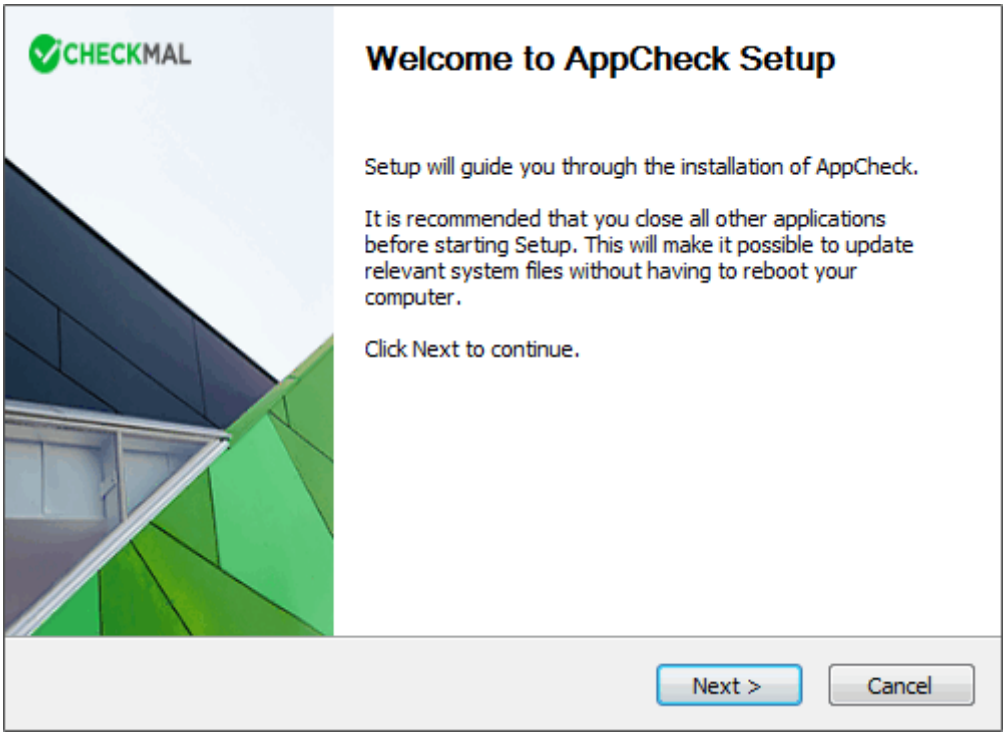


In precedenza avevo recensito il programma **Cybereason RansomFree**, purtroppo l'azienda che lo produceva ha interrotto la distribuzione. In passato avevo provato anche **AppCheck Anti-Ransomware**, non lo recensii perché se non ricordo male aveva solo un breve periodo di prova, ora invece è diventato

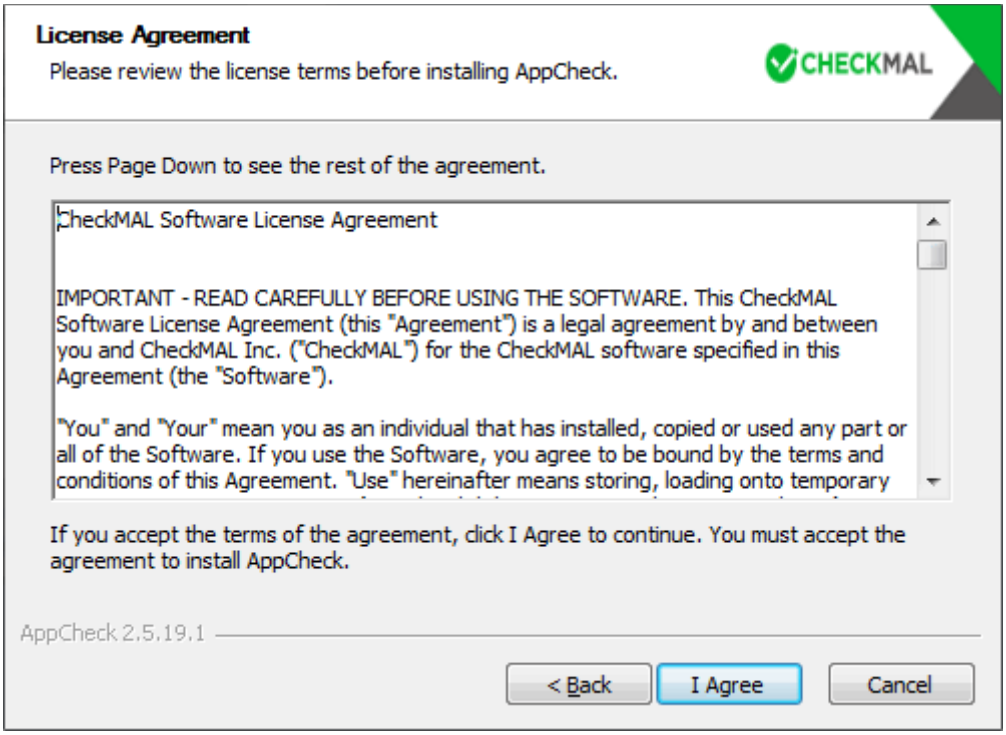
gratuito con delle limitazioni. Vediamo come funziona.

Installazione

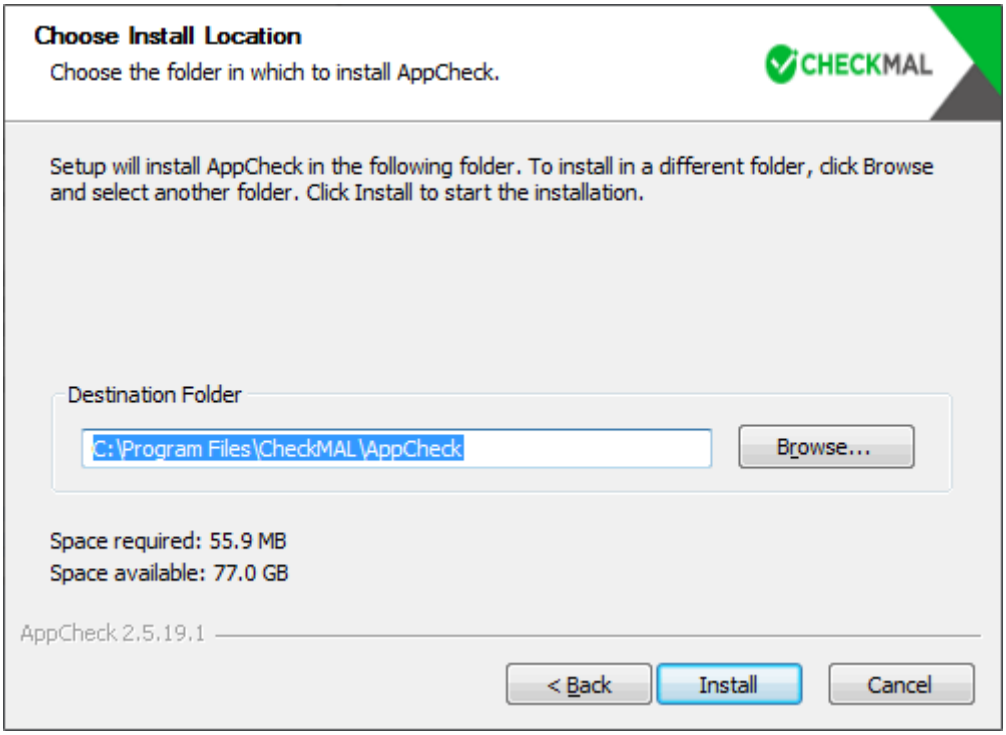
Lanciamo il programma e clicchiamo su **Next**



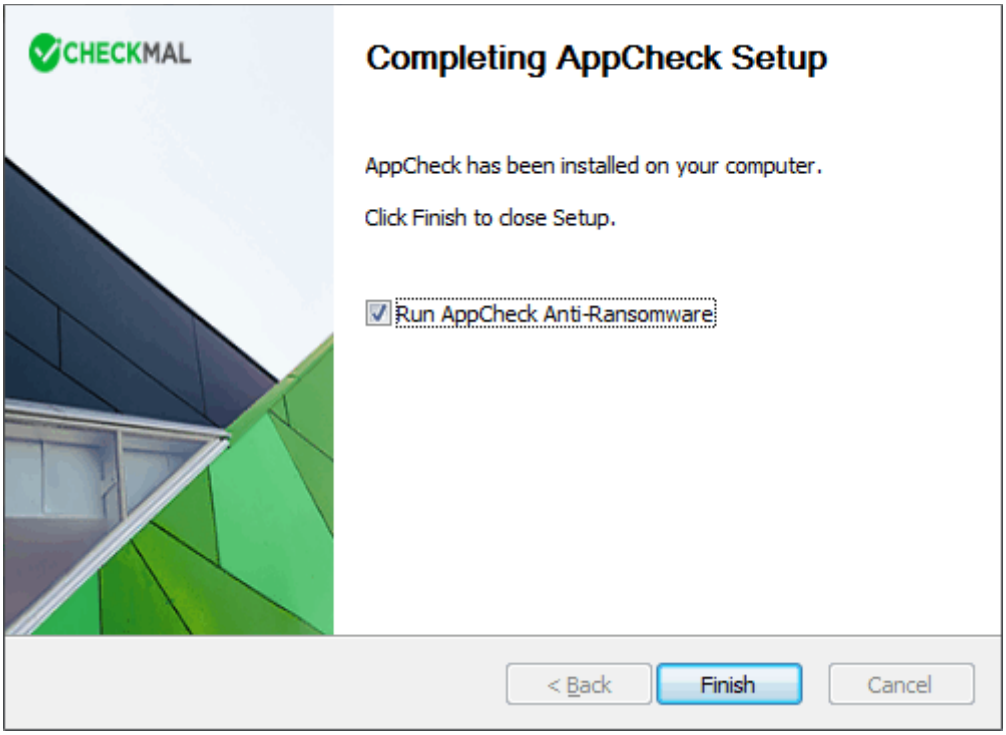
Clicchiamo su **I Agree**



Clicchiamo su **Install**

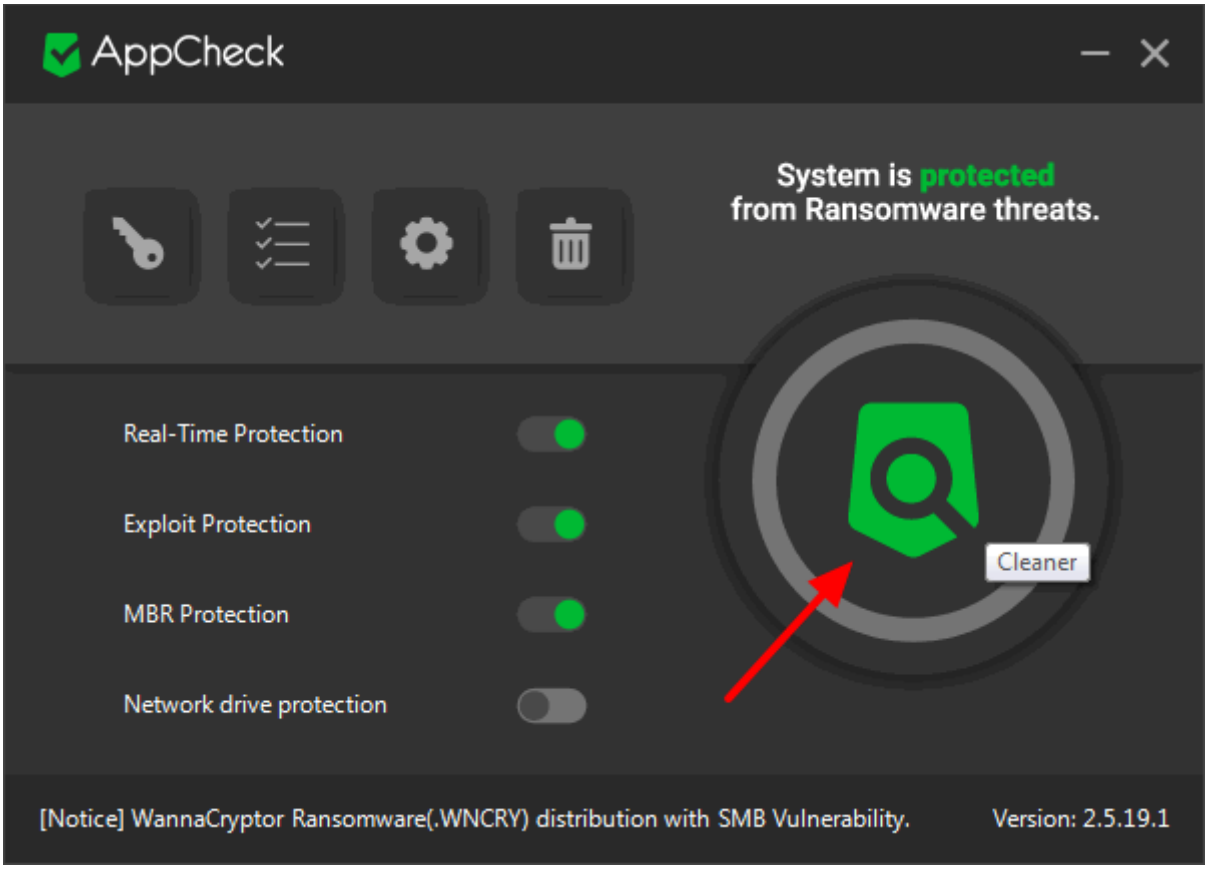


Clicchiamo su **Finish**

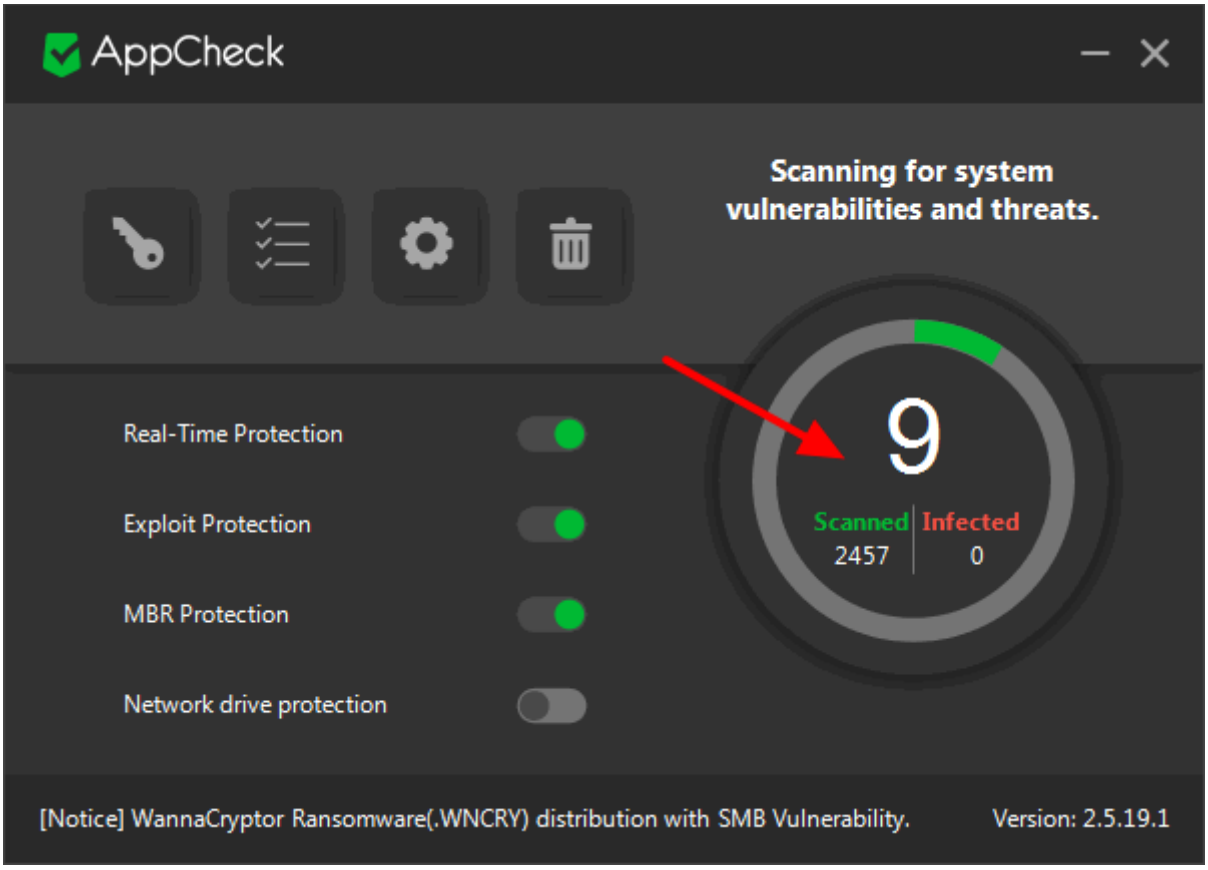


Descrizione

Questa è la schermata di AppCheck, iniziamo col fare una scansione Anti-Spyware, clicchiamo sul cerchio per lanciare **Cleaner**

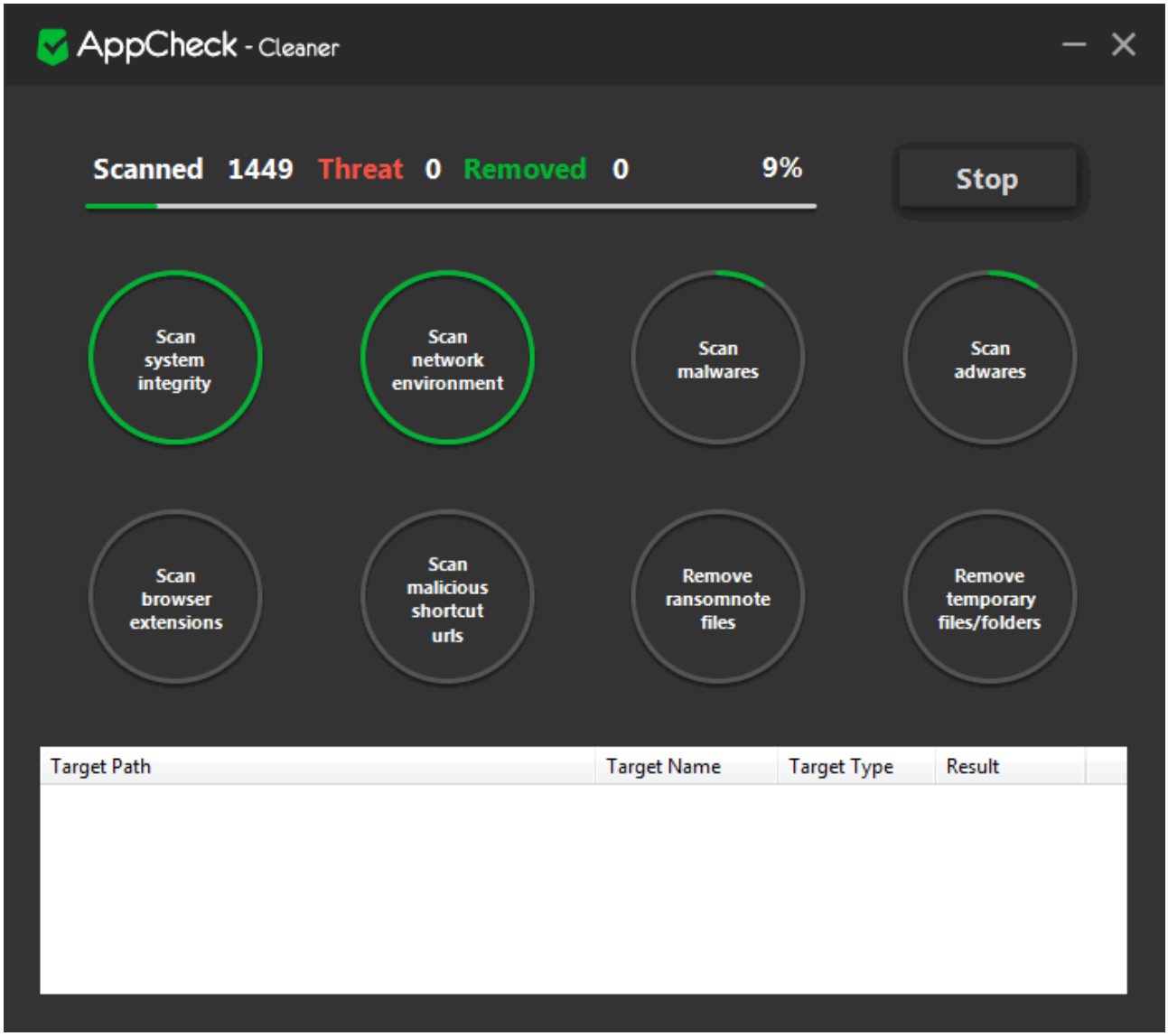


Inizia subito la scansione, clicchiamo una seconda volta sul cerchio



Si aprirà questa schermata con la scansione di varie tipologie di malware.

La scansione di tutte le aree non è molto lunga, più o meno come la scansione veloce di un Antivirus per i soli file di sistema.

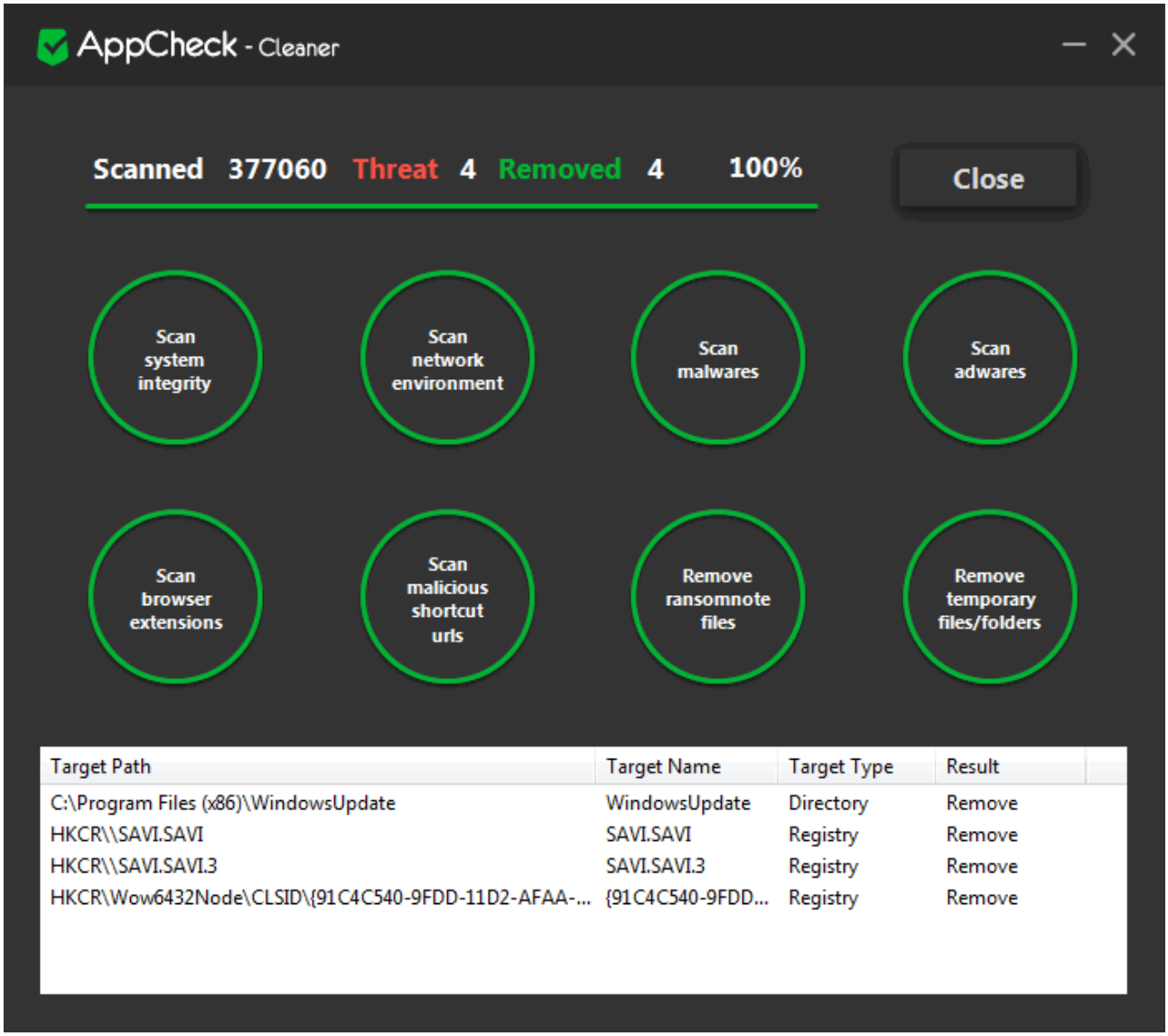


Ed ecco qui il rapporto a fine scansione. Nel mio sistema c'erano 4 malware da rimuovere.

Purtroppo ha eliminato anche la cartella del Windows Update, ehi sto scherzando, il Windows Update non ha una cartella, si trova in **C:\ Windows\ System32** e il file per lanciare il Windows Update si chiama **wuapp.exe**.

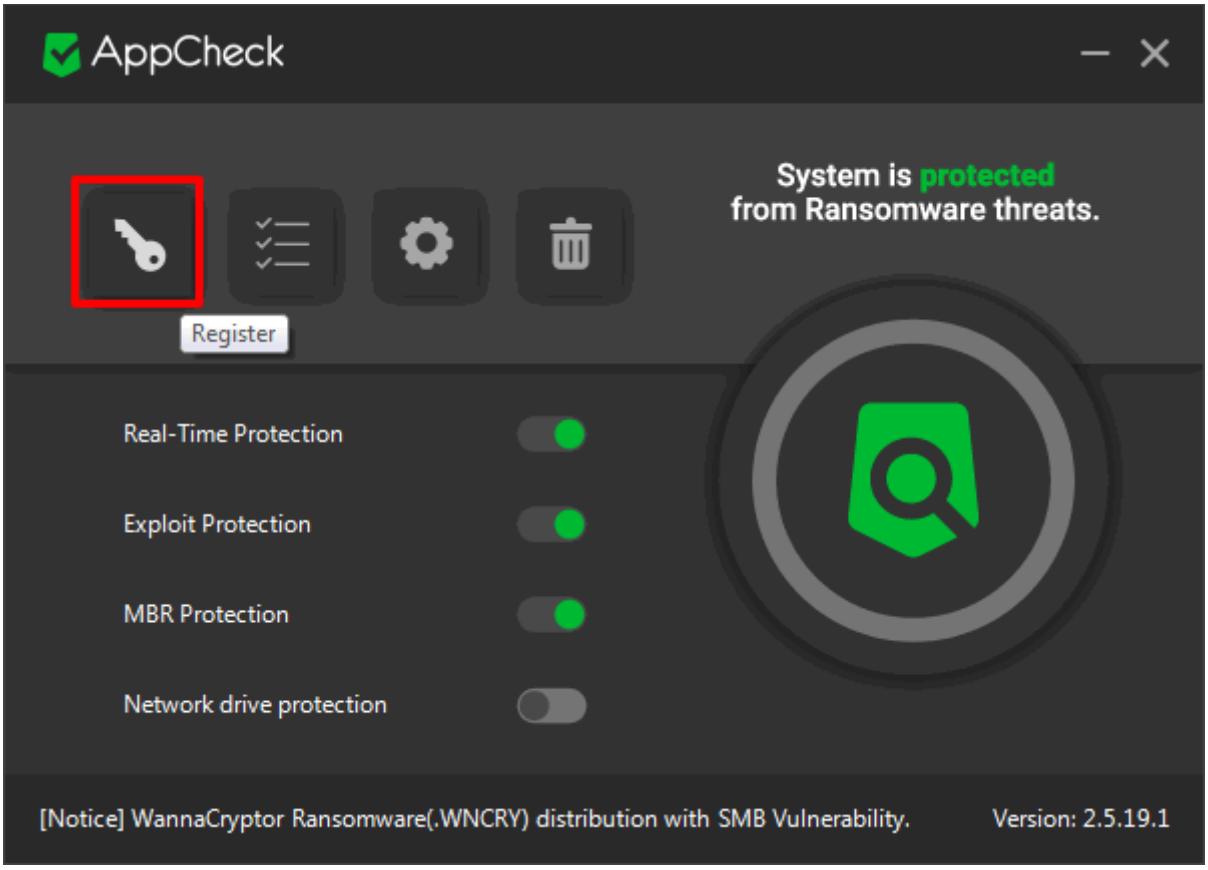
La cartella **Windows Update** che ha eliminato era una minaccia al 100%, in più ha rimosso altre tre voci dal registro e messo il tutto in quarantena.

Nel caso la scansione non rileva alcuna minaccia, questa finestra si chiude entro cinque secondi, se ci sono minacce resta aperta. Chiudiamo la finestra.



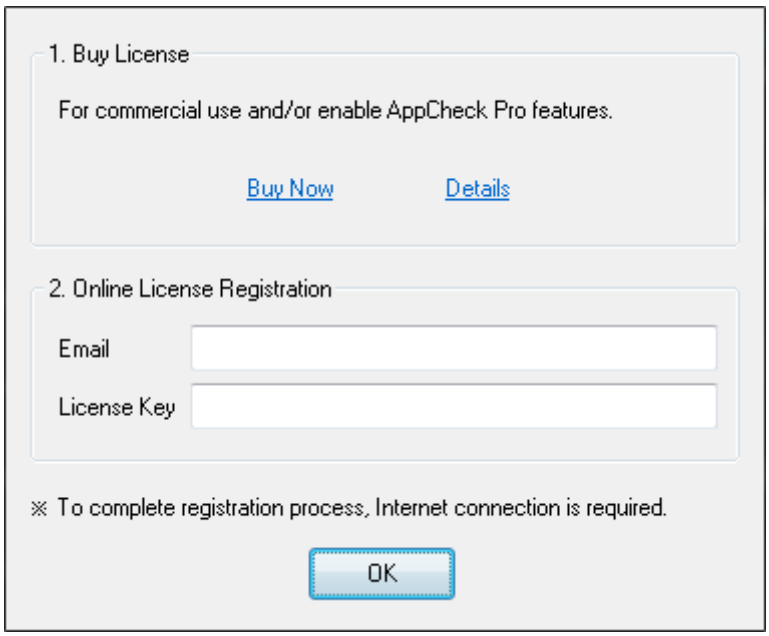
Vediamo gli altri pulsanti:

Register, serve per acquistare o aggiornare una licenza PRO al costo di 39 Dollari annuali.

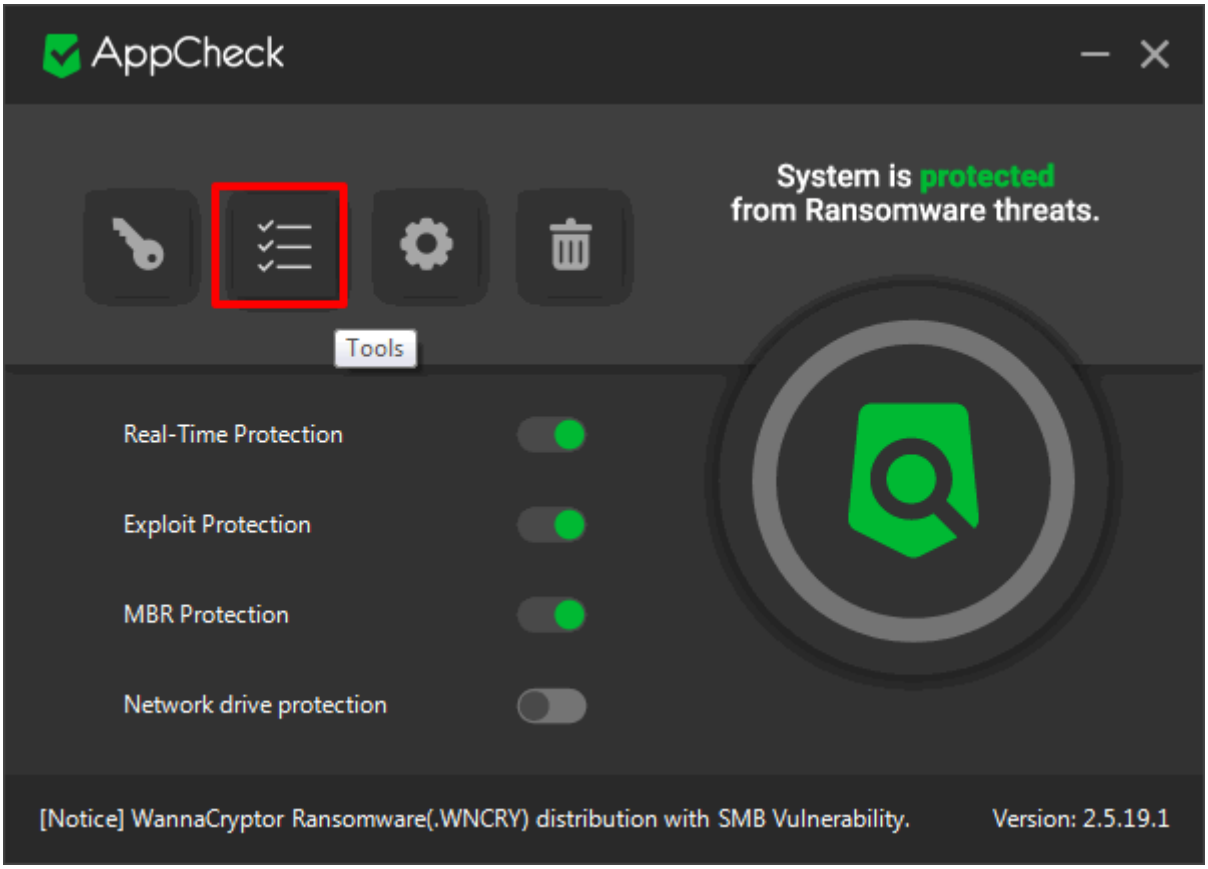


Cliccando sull'icona **Chiave** la si apre questa finestra, cliccando su **Buy Now** si acquista una licenza, una volta ricevuto la chiave della licenza si deve inserire indirizzo e-mail e il numero di licenza per attivarlo.

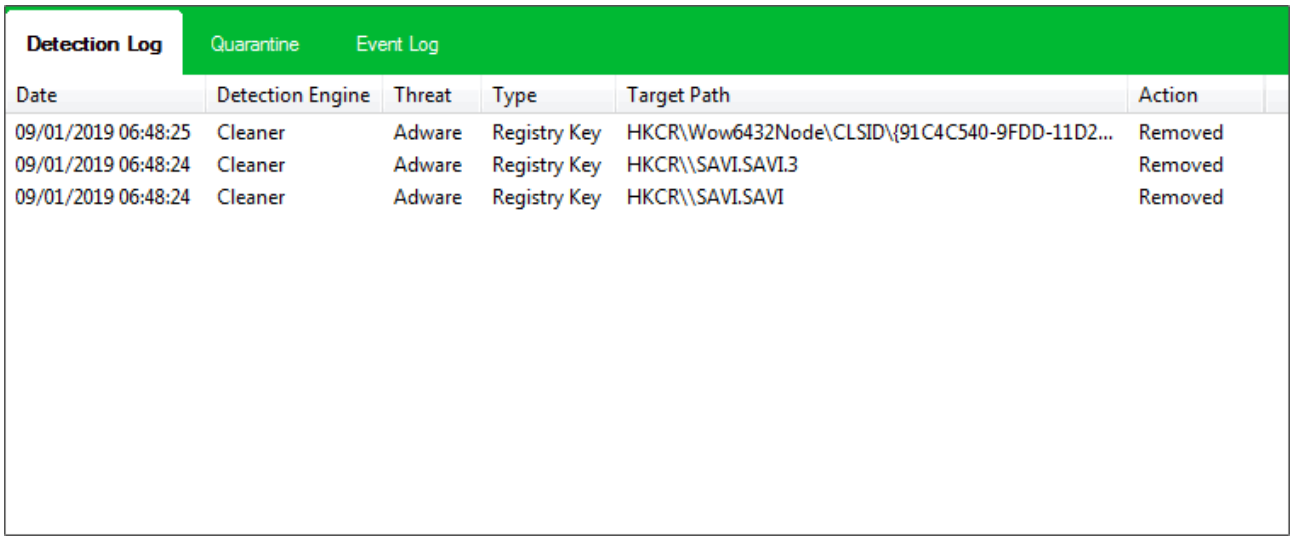
Noi continuiamo a spiegare la versione gratuita.



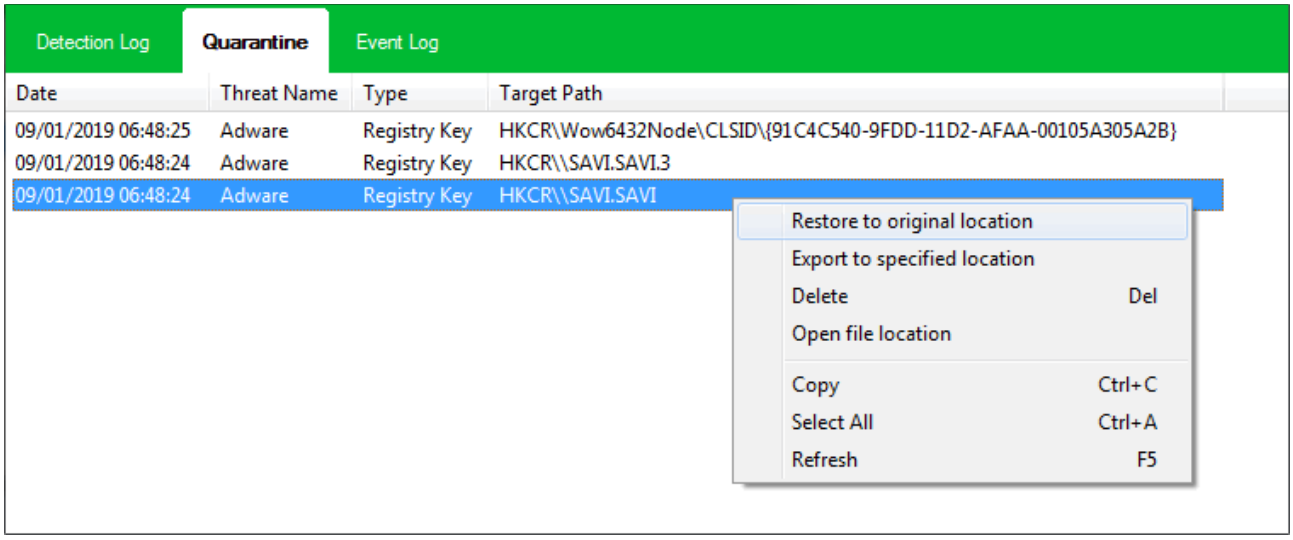
Cliccando il secondo pulsante **Tools** si accede alla Quarantena.



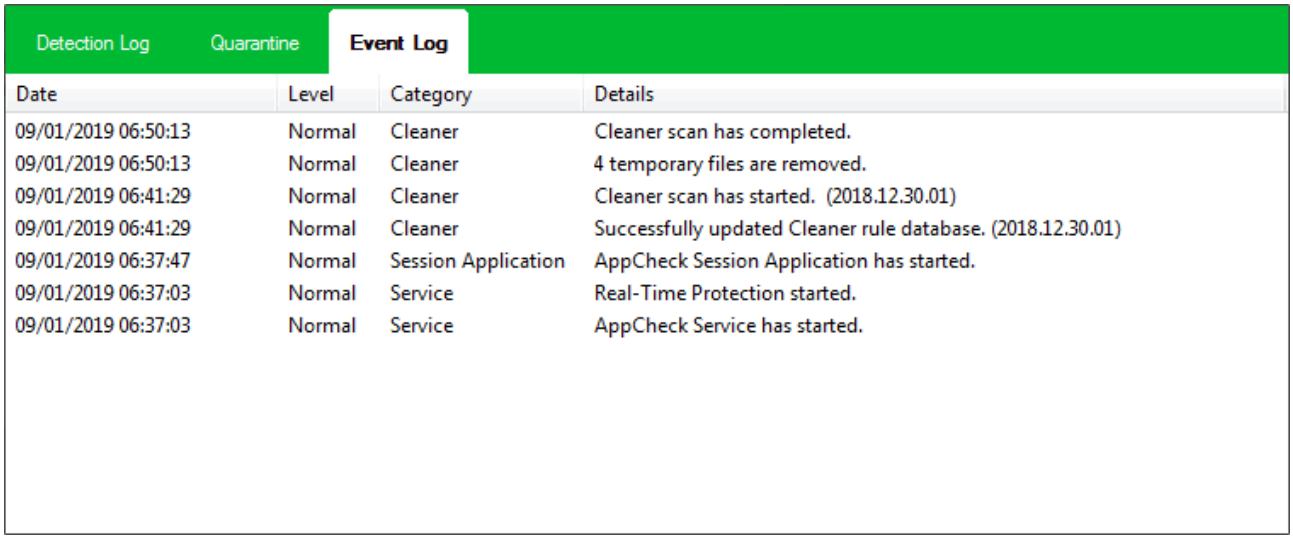
In **Deletion Log** troviamo le voci eliminate



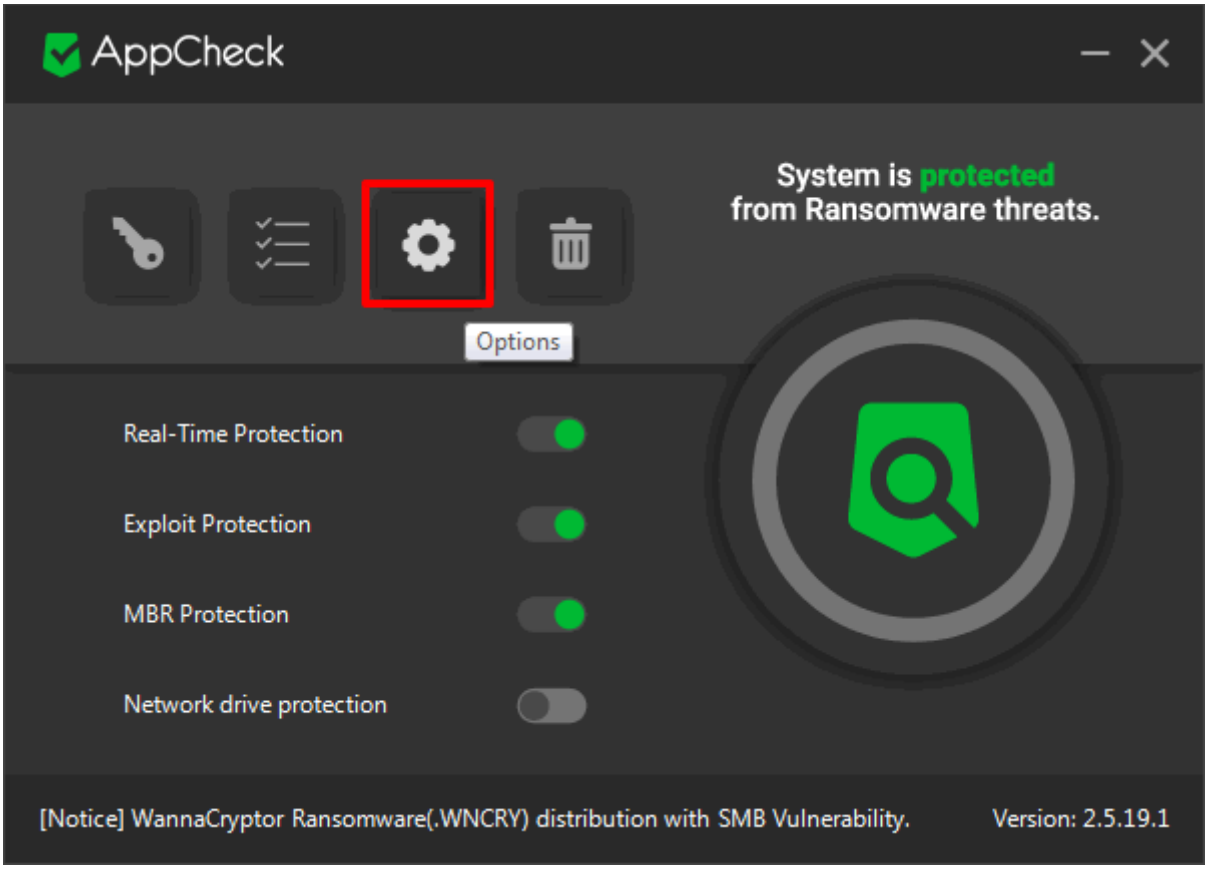
In **Quarantine** possiamo ripristinare file e voci eliminate, nel caso siamo sicuri che non siano malware.



Event Log mostra tutte le azioni all'interno del programma, inclusi gli aggiornamenti del programma e del database spyware del Cleaner.



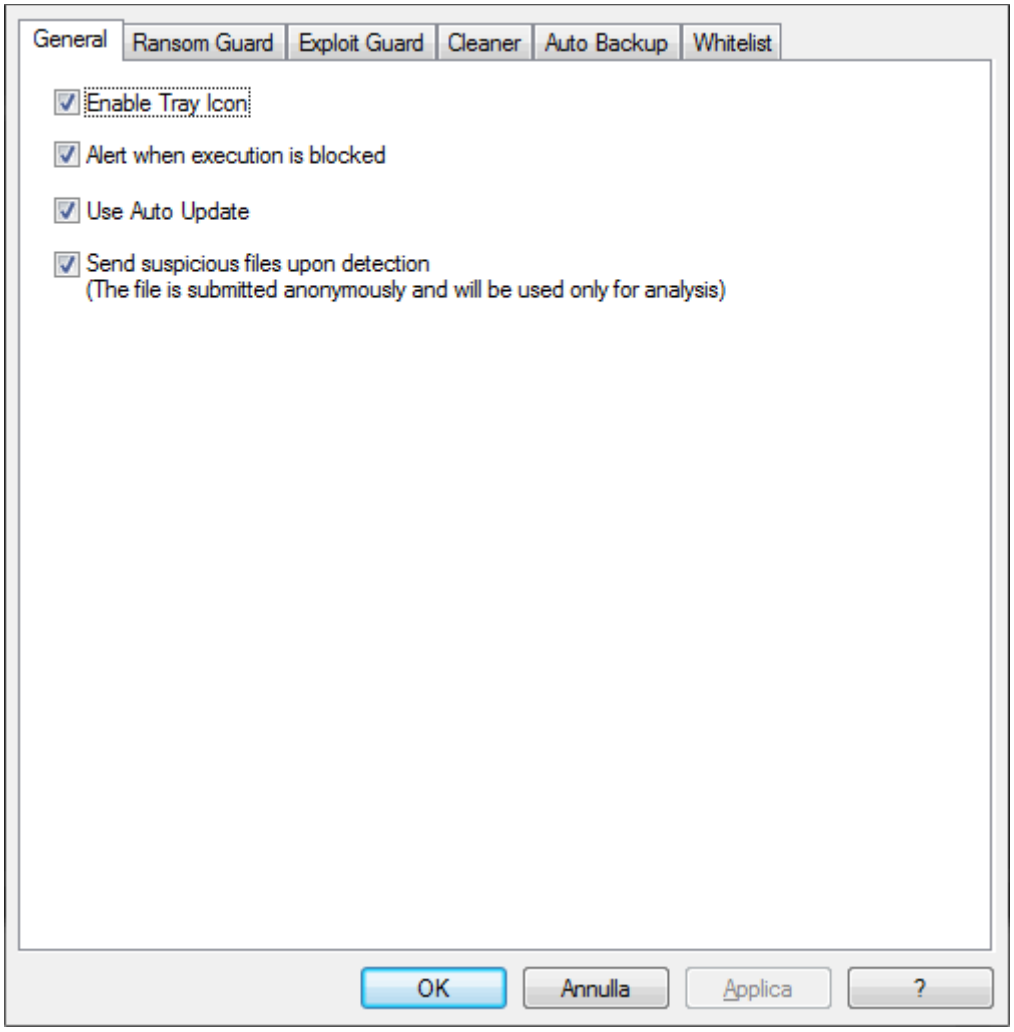
Il terzo pulsante **Options** riguarda le impostazioni



Vediamole tutte

General

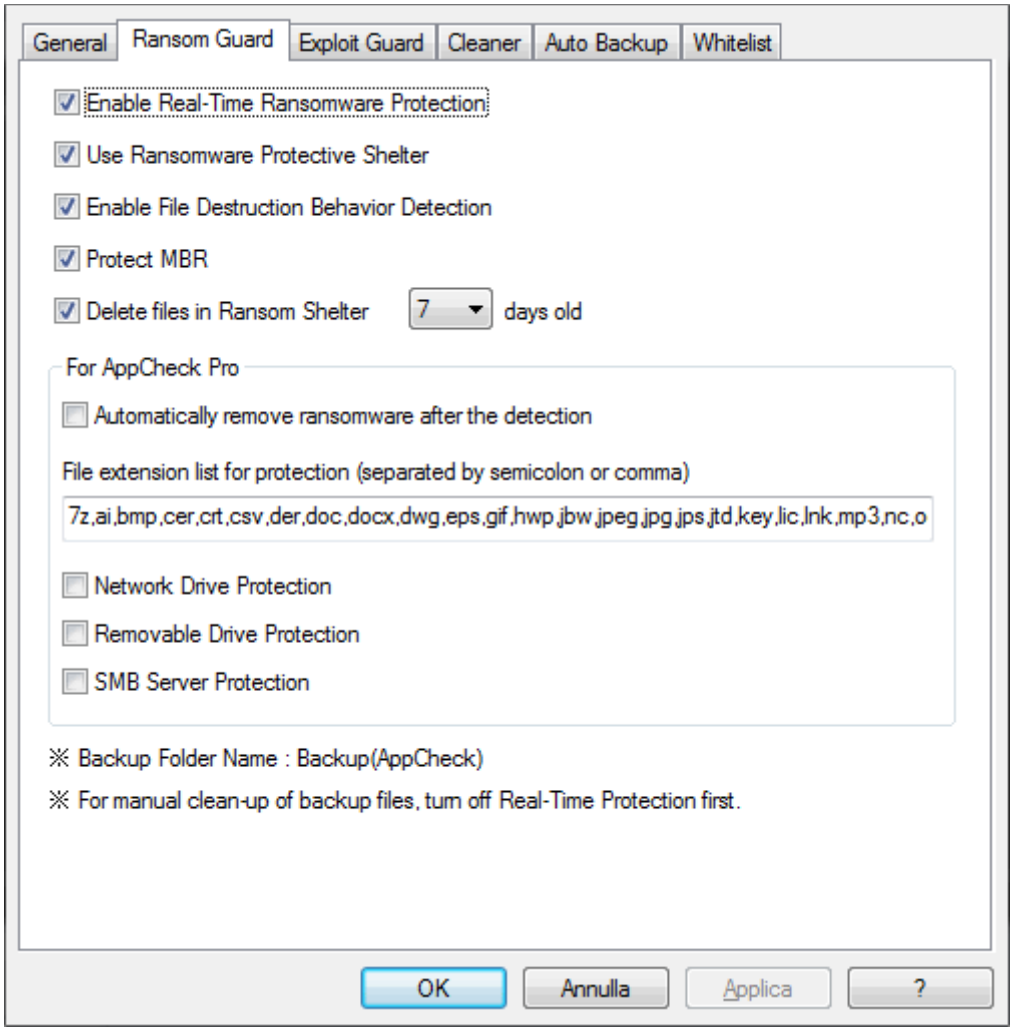
- Enable Tray Icon
  Possiamo abilitare o disabilitare la visione dell'icona nella barra applicazioni.
- Alert when execution is blocked
  Ci avvisa se il programma è stato bloccato da un malware
- Use Auto Update
  Il programma si aggiorna in automatico
- Send suspicious files upon detection
  Invia i file ritenuti sospetti per le analisi



Ransom Guard

- Enable Real-Time Ransomware Protection
  Attiva la protezione in tempo reale
- Use Ransomware Protective Shelther
  Utilizza la cartella protetta per i file modificati
- Enable File Destruction Behavior Detection
  Attiva il rilevamento contro la modifica dei file
- Protect MBR
  Protegge la MBR dalle modifiche dei malware
- Delete files in Ransom Shelter selezionare da **1** a **7** giorni
  Elimina i file protetti dopo i giorni impostati (lo vediamo in seguito)

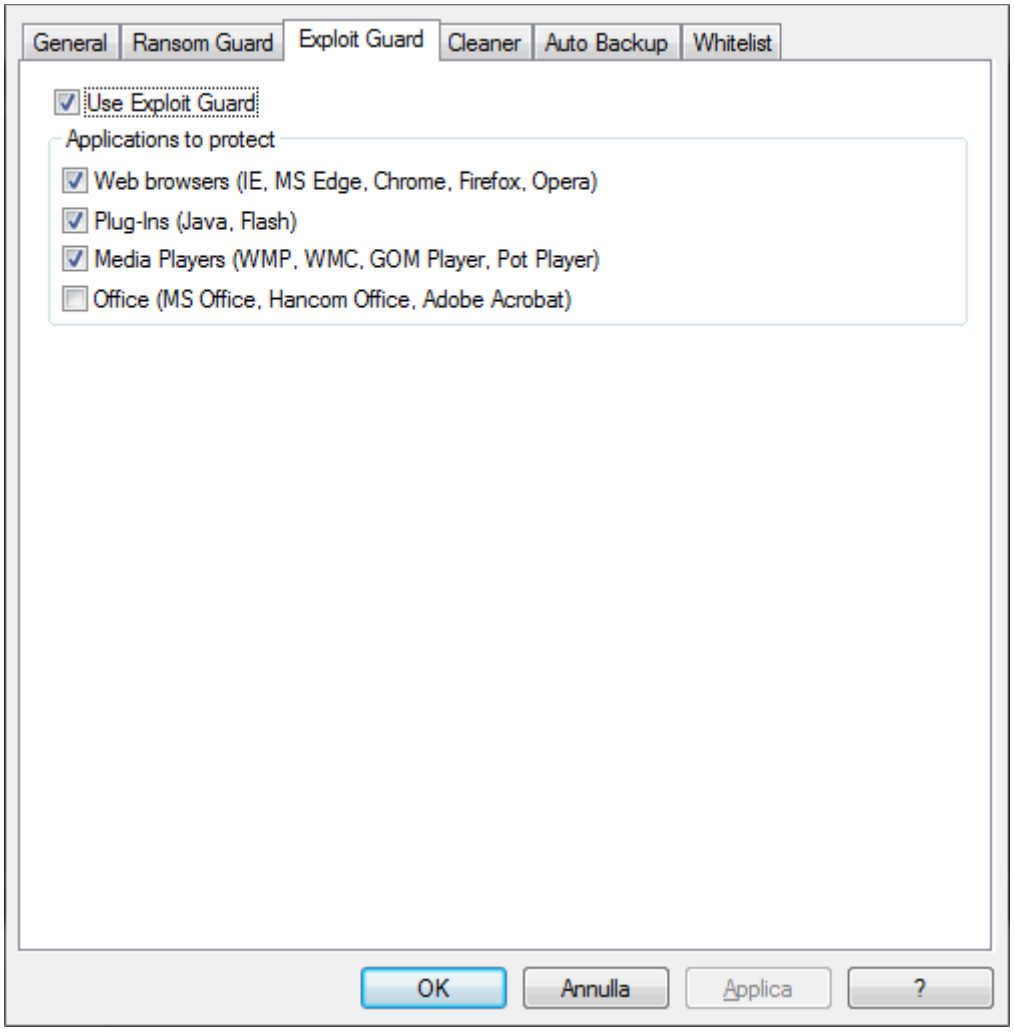
Le altre voci riguardano la versione **PRO**, in sostanza, la versione gratuita protegge il sistema e fa la copia di backup di tutti i file modificati, ma non ripristina in automatico i file modificati dal ransomware come fa la versione PRO. Nel caso il programma blocca una minaccia, dovremo ripristinare manualmente i file dal backup. Sempre meglio che nulla, non credete?



Exploit Guard

Un **Exploit**, che significa "Sfruttare" è un termine usato in informatica per identificare una tipologia di script, virus, worm, porzione di dati o binario che sfrutta un bug o una vulnerabilità per creare comportamenti non previsti in software, hardware, o in sistemi elettronici.

- Use Exploit Guard
  Attiva la protezione da Exploit per **Web Browser**, **Plug-Ins** e **Media Player**
- Per software tipo **Office** necessita la versione PRO



Cleaner

- Scan System Integrity
  Modifica di tutti gli elementi relativi a OSF Windows come file modificati o registro o richiedere il riavvio di Windows se necessario.

- Scan network environment
  Controlla le informazioni di configurazione di rete del sistema e modificarlo se presenta impostazioni dannose.

- Scan malwares
  Rimuove i programmi dannosi se è installato sul tuo sistema.

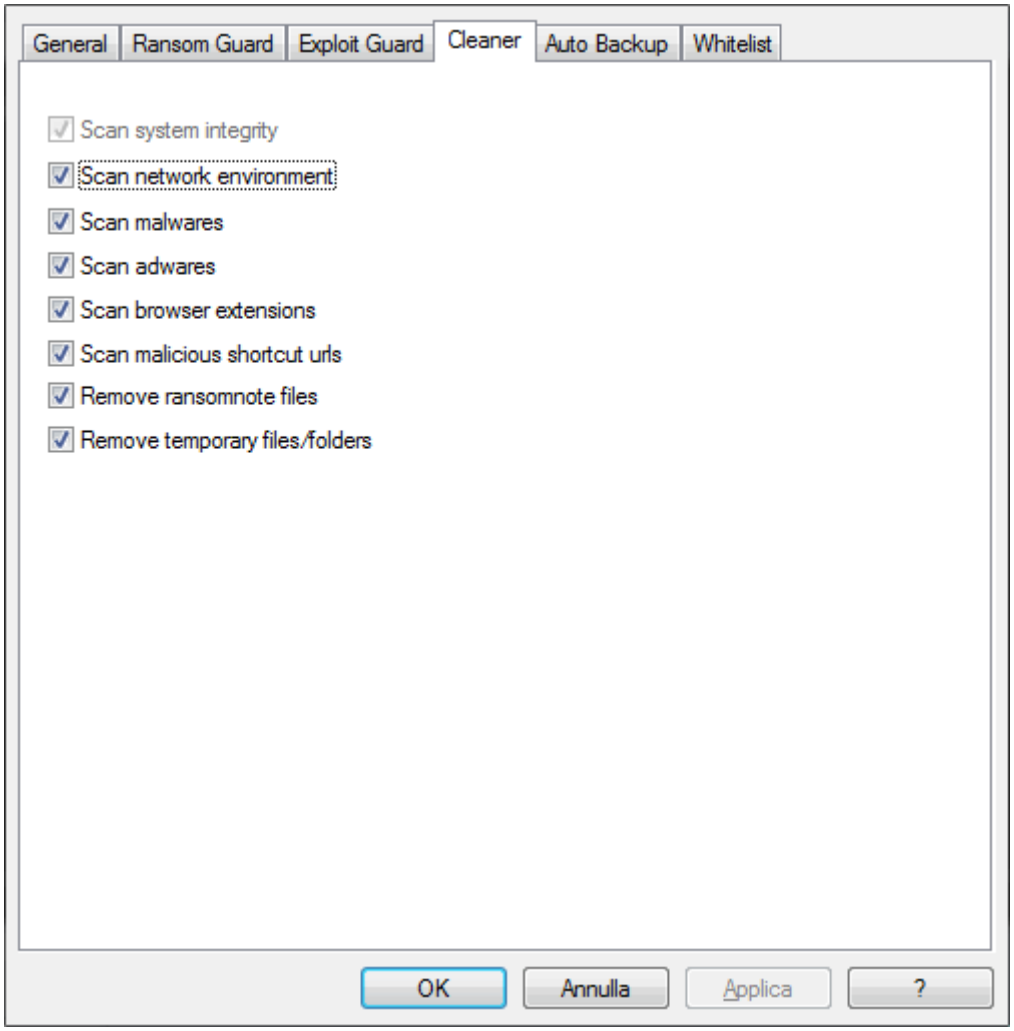
- Scan adwares
  Rimuove i programmi pubblicitari installati sul tuo sistema che potrebbero causare inconvenienti.

- Scan browser extension
  Rimuove le estensioni pericolose dal browser.

- Scan malicious shortcut urls
  Rimuove i collegamenti sul desktop o nell'area Preferiti se si connette a un sito dannoso.

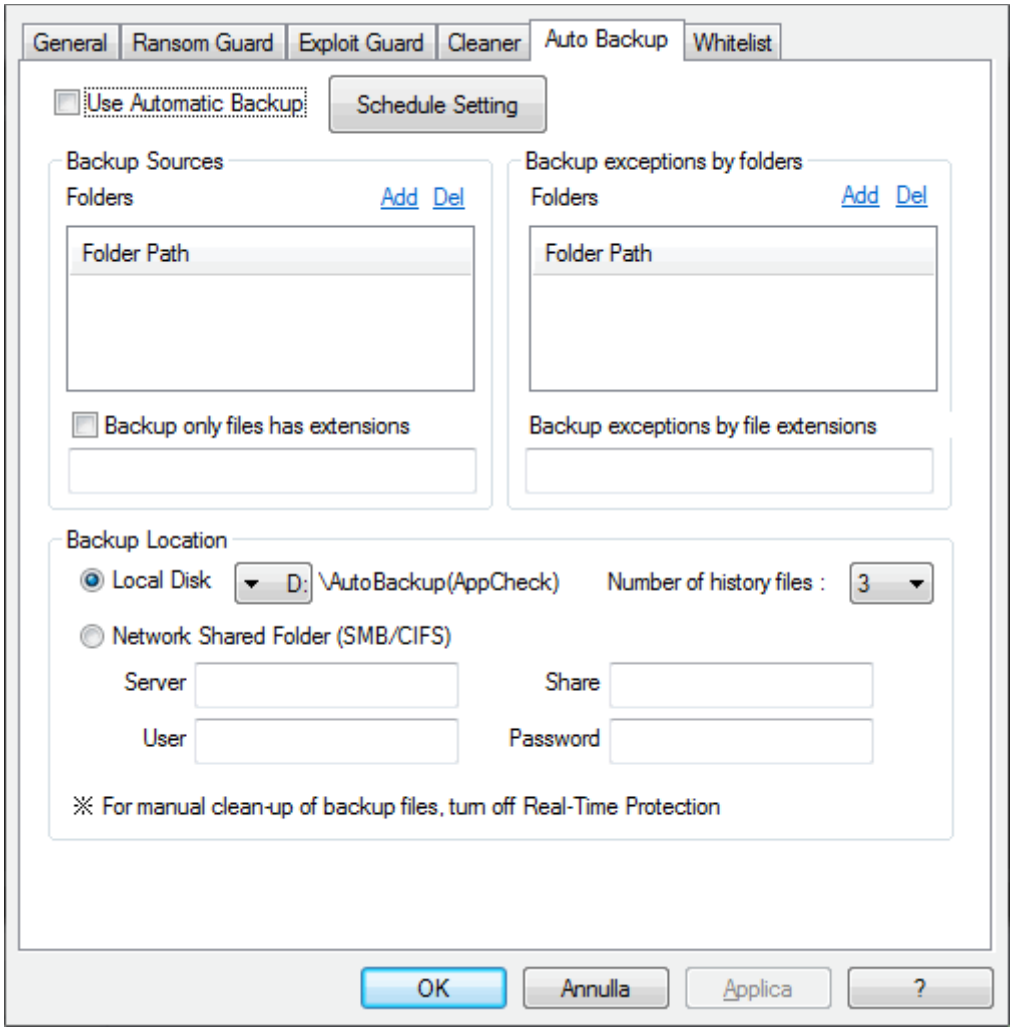
- Remove ransomnote files
  Rimuove qualsiasi file di guida ai pagamenti generato dall'infezione da ransomware.

- Remove temporary file/folders
  Rimuove file e cartelle non necessari presenti nella cartella temporanea



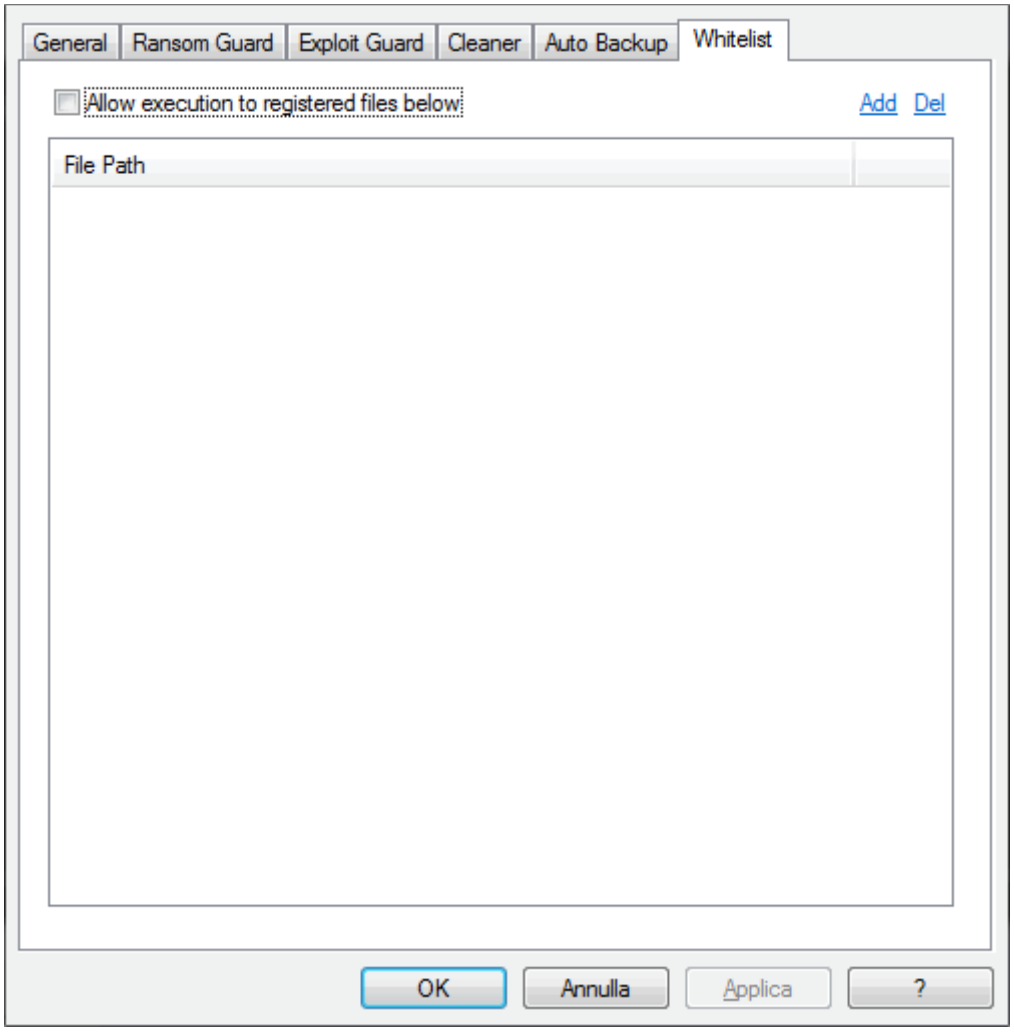
Auto Backup

Funziona solo sulla versione PRO

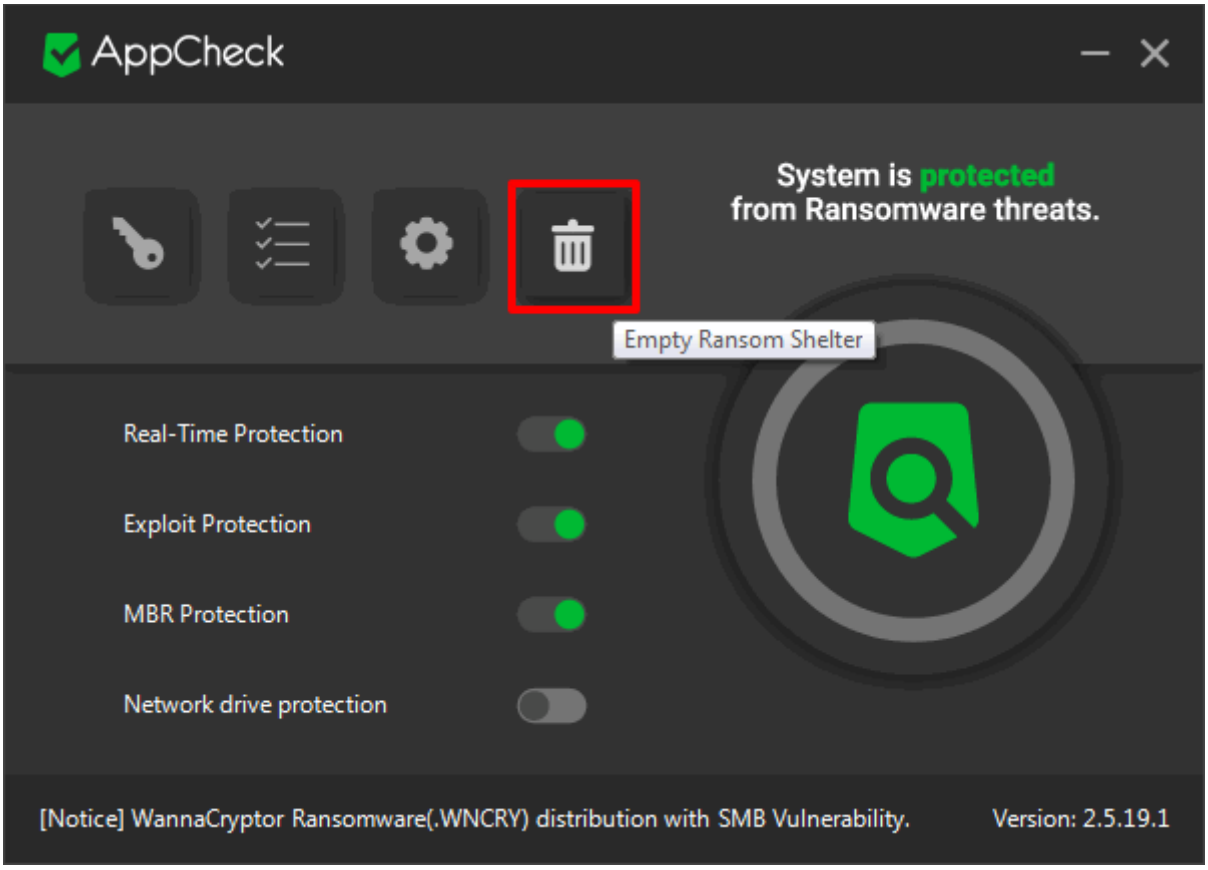


Whitelist

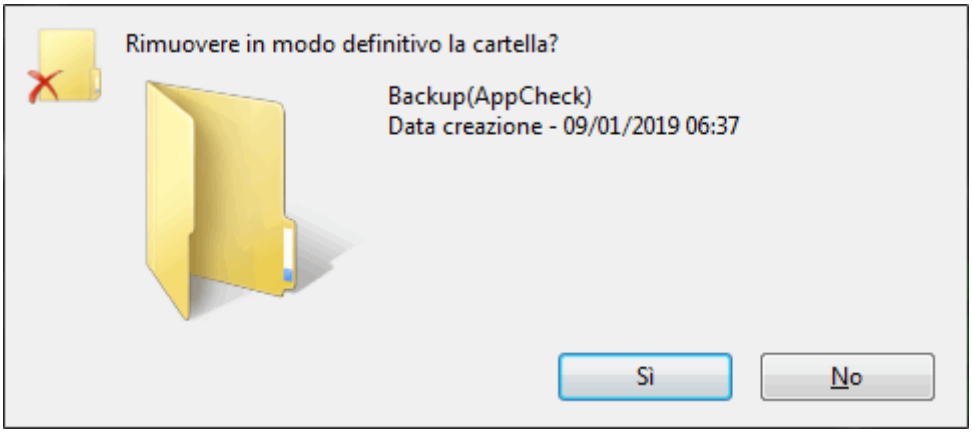
La whitelist è una funzionalità che consente agli utenti di aggiungere file bloccati dal rilevamento delle attività ransomware, falsi positivi.



Il quarto pulsante **Empty Ransom Shelter** permette di eliminare la cartella di Backup



Cliccando l'icona Cestino compare questa finestra che chiede la conferma per eliminare il backup dei file, se nel nostro sistema ci sono più partizioni comparirà una finestra per ogni partizione.



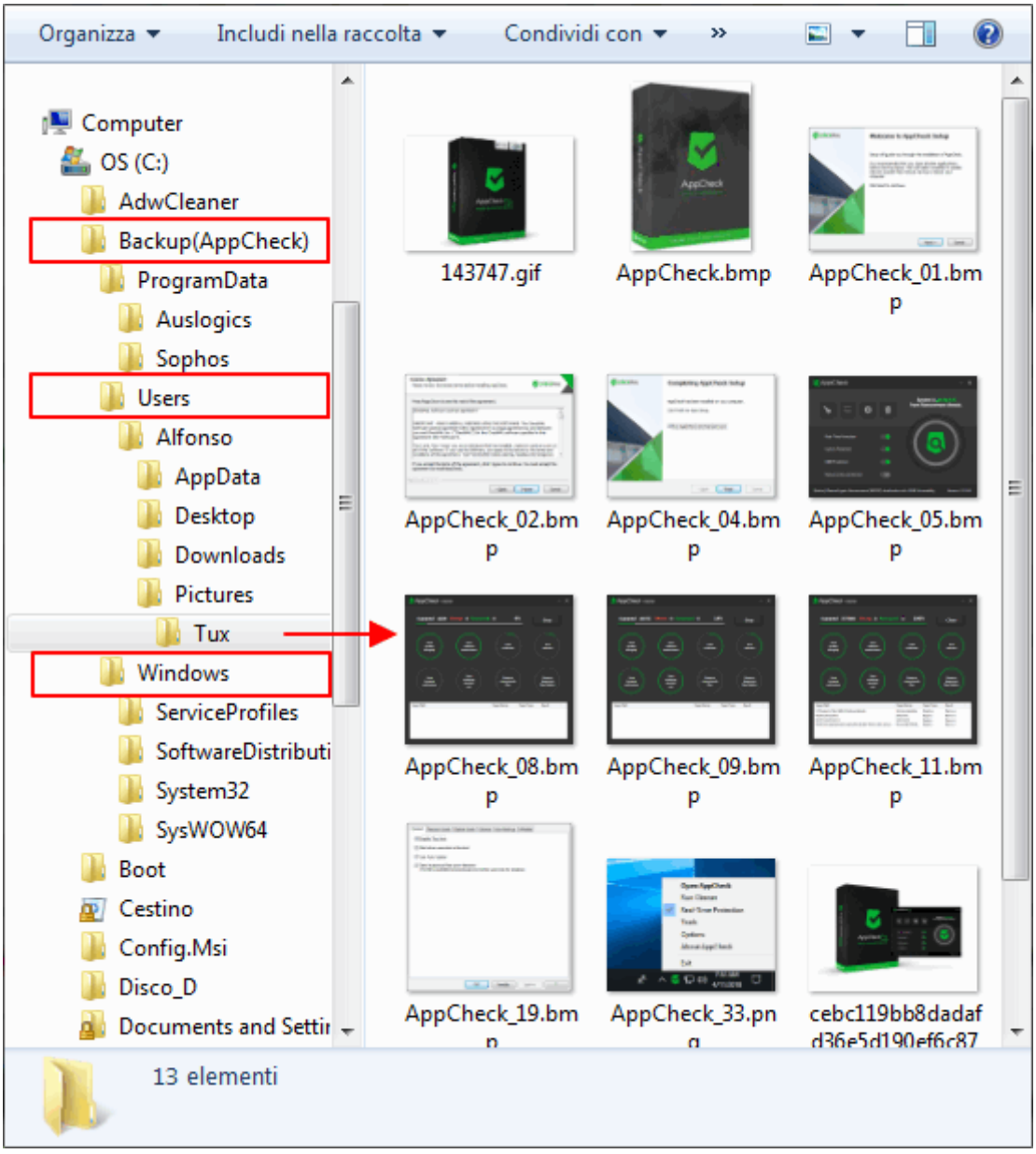
AppCheck crea in ogni partizione una cartella dal nome **Backup(AppCheck)** quando in quella partizione viene modificato anche un solo file.

Come ho già detto in altri articoli, quando un file viene modificato, il vecchio file non viene mai soprascritto, viene cancellato e creato un nuovo file con la modifica.

Quando un file viene modificato da un Ransomware, il file originale viene eliminato, quindi tecnicamente potrebbe essere recuperato, il problema è che se il sistema è infetto verrebbe infettato anche il file recuperato.

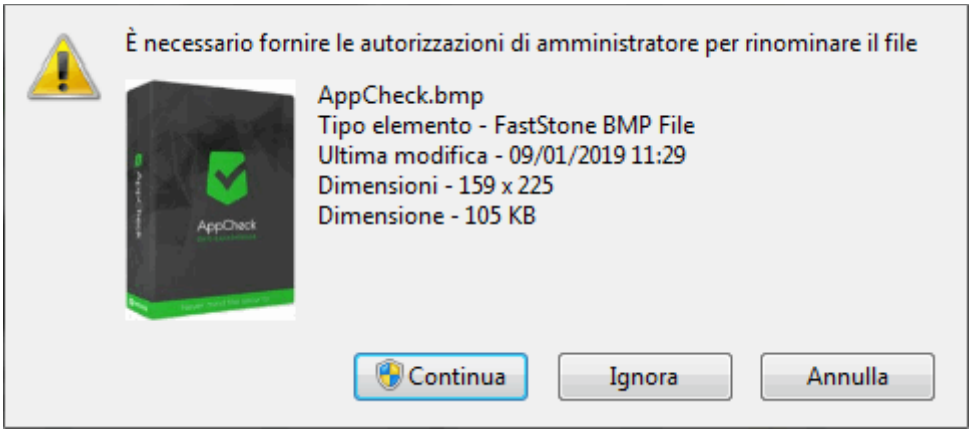
AppCheck protegge i file eliminati inserendoli nella cartella Backup con i percorsi appartenenti ai file eliminati. Qui sotto vediamo un esempio, le immagini sono relative alla realizzazione di questa guida, dopo averle salvate in GIF ho eliminato i BMP più pesanti.

Dalla cartella Backup possiamo prendere i file che ci interessano e copiarli nei percorsi originali, ma non possiamo ne spostarli, ne rinominarli, ne cancellarli, la cartella e protetta da AppCheck



Se proviamo a rinominare, cancellare o modificare un file compare questo messaggio, anche dando la conferma il file non può essere eliminato in alcun modo.

Tranquilli esiste un modo per eliminare i file manualmente, vedi immagine successiva.



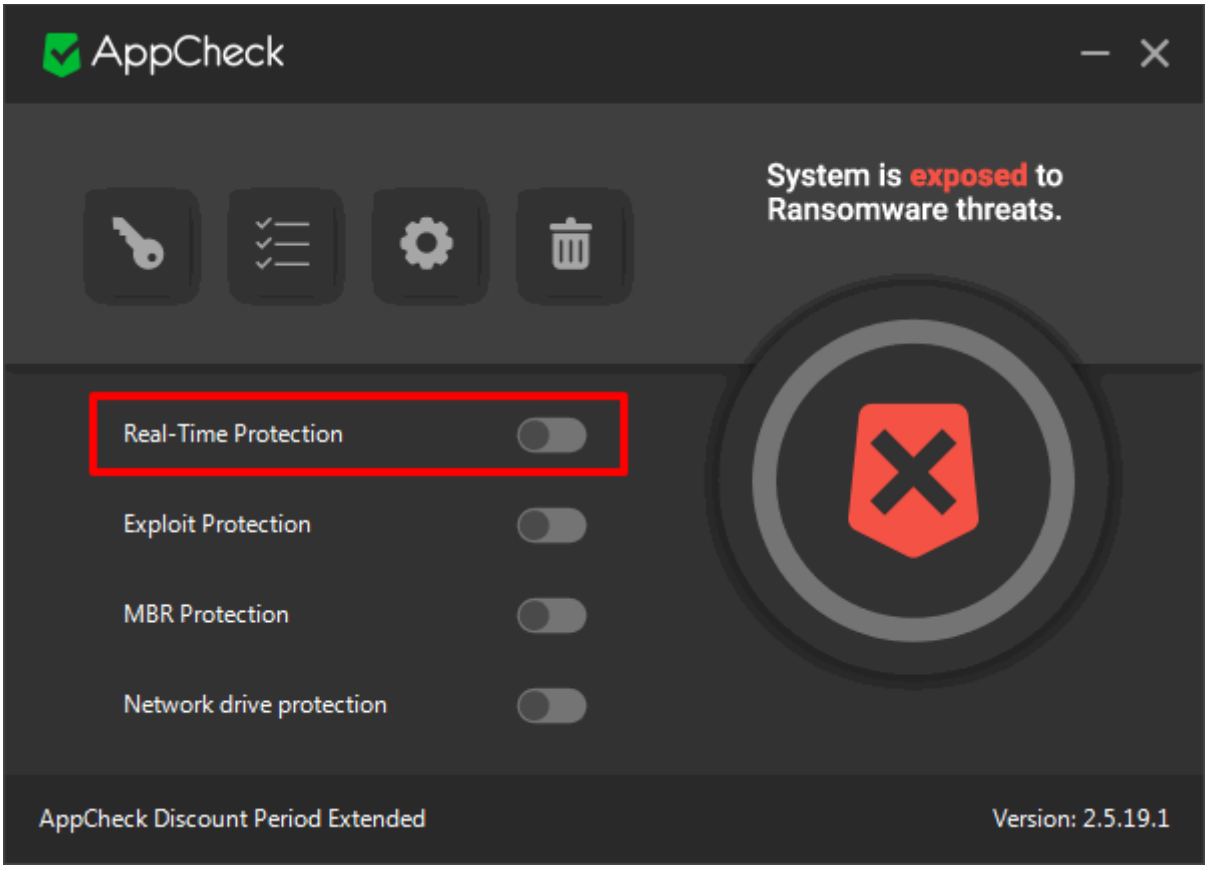
Come già detto, per eliminare tutti i backup basta cliccare sull'icona Cestino.

Ma se, ad esempio, facciamo una copia dei dati giornaliera con **FBackup** senza togliere la spunta alla cartella **Backup(AppCheck)** in Proprietà - Sorgenti di FBackup, questo lo includerà nella copia di riserva.

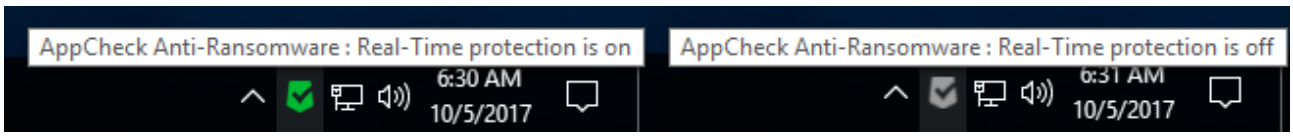
La cartella **Backup(AppCheck)** può arrivare a contenere centinaia di Mbyte di dati o anche più, e copiare anche questi sarebbe una perdita di tempo oltre al consumo di spazio sul disco esterno. In pochi giorni che utilizzo AppCheck la cartella backup è arrivata a quasi 20 Mbyte, ed era stata copiata anche nel disco esterno.

Per rimuovere una cartella **Backup(AppCheck)** dal disco esterno bisogna disattivare la protezione in tempo reale, cliccando su **Real-Rime Protection**, eliminata la cartella riattiviamolo subito.

Il bello di AppCheck è che questa protezione funziona anche contro i virus che modificano i file o per recuperare un file nel caso lo abbiamo modificato e salvato per errore.

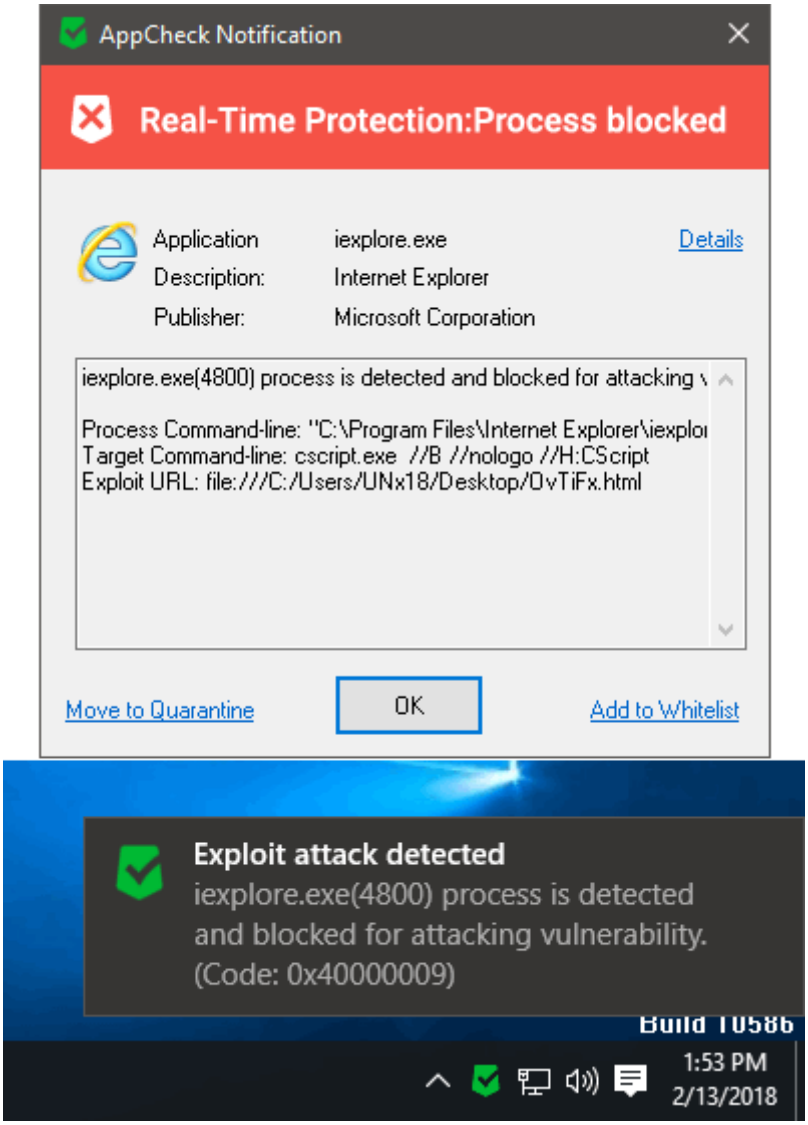


Quando AppCheck è disattivato l'icona da verde diventa grigia.

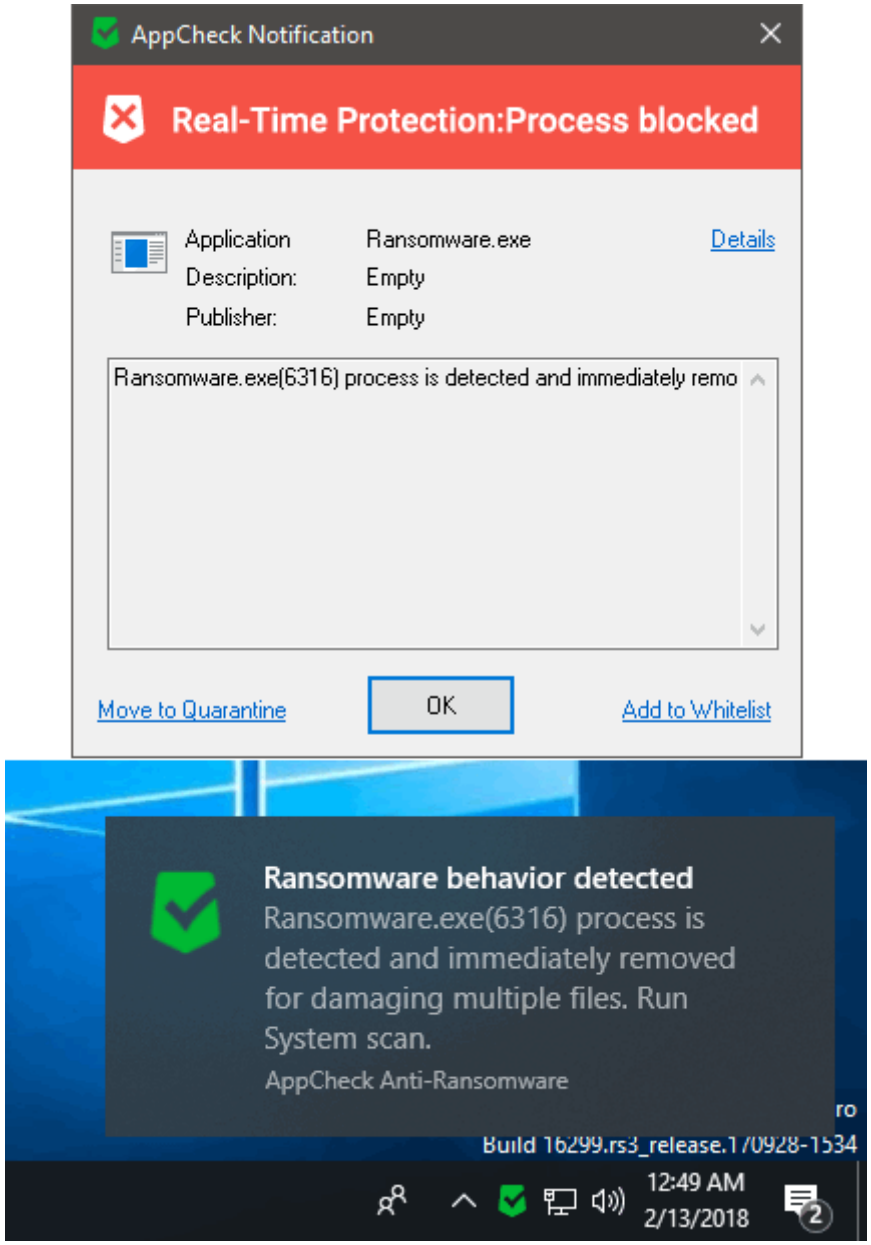


Non avendo mai avuto problemi di Ransomware, ho rubato qualche immagine al sito del programma :o)

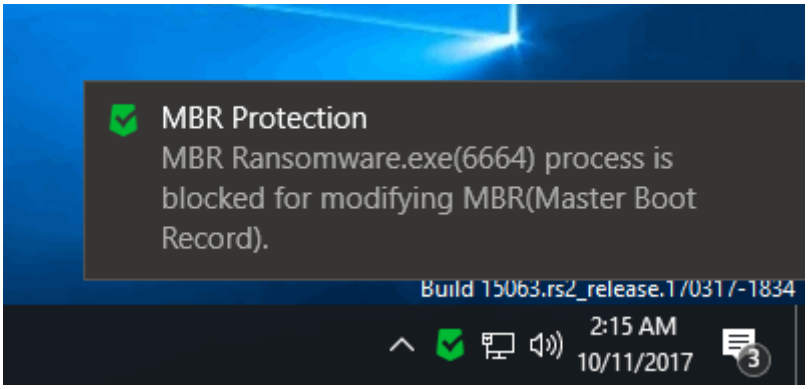
Questo è un avviso di minaccia da Exploit su Intenet Eplorer, bloccato in tempo reale da AppCheck



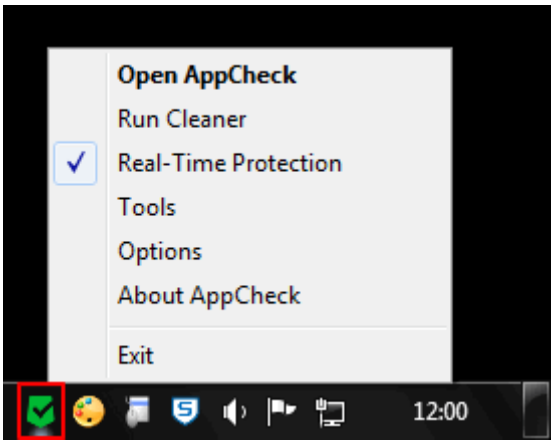
Questo e un avviso di attacco Ransomware, bloccato in tempo reale da AppCheck



Questo e un avviso di attacco alla MBR, bloccato in tempo reale da AppCheck



Si può accedere alle funzioni di AppCheck anche senza aprire il pannello, ad esempio per lanciare Cleaner, selezioniamo l'icona con il pulsante destro del mouse e spuntiamo la voce che ci interessa.



Conclusioni

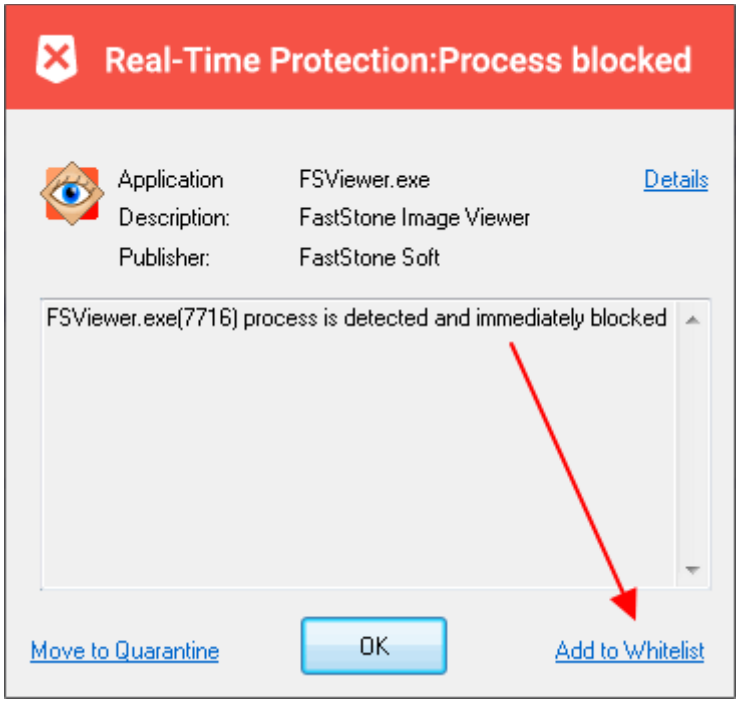
AppCheck non fa il controllo in tempo reale sui file che contengono Ransomware come gli Antivirus, potete scaricare un file infetto da Ransomware, AppCheck lo intercetta e blocca solo quando entra in esecuzione, quindi non necessita di alcun aggiornamento definizioni come gli Antivirus. Per questo motivo non solo e compatibile con qualsiasi Antivirus ma lo aiuta nella protezione del sistema. Come già detto se un virus provasse a modificare un file, l'antivirus rimuoverebbe il virus e AppCheck proteggerà il file, che se danneggiato potrà essere recuperato dalla cartella di Backup, inoltre fa anche la scansione anti-spyware. Pertanto lo consiglio a tutti.

E vero consuma un po' di spazio su disco salvando qualsiasi cosa venga modificato, ma se abbiamo poco spazio possiamo impostare la cancellazione automatica a **un giorno** invece che a **sette giorni**, (vedi in **Opzioni - Ransom Guard**) e in ogni caso possiamo eliminare i backup in qualsiasi momento per recuperare spazio in caso di bisogno, ma il bello è proprio avere una copia di riserva nel caso entra qualche manigoldo di virus o altro malware nel nostro sistema a fare qualche festino non autorizzato.

Voce aggiunta

Stavo salvando diverse immagini da BMP a GIF e l'operazione è stata vista come malevole, AppCheck ha bloccato il programma FastStone Image View, cancellato tutte le immagini GIF e ripristinato le immagini BMP che avevo cancellato una per una dopo averle salvate in GIF. Purtroppo mi tocca risalvare tutte le immagini in GIF, ma è una buona notizia, significa che fa anche il ripristino dei dati in automatico se vengono modificati da un Ransomware.

Se vi succede la stessa cosa con qualche programma, dovete cliccare su **Add Whitelist** per impedire che accada di nuovo. Se usate qualche programma per svolgere operazioni ripetitive, aggiungetelo alla Whitelist.



::: Fine Guida - AppCheck Anti-Ransomware